



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,948	02/19/2002	John M. Haltmeyer	HALTMEYER-PA-2	3414

7590

10/05/2005

LAW OFFICES OF ROYAL W. CRAIG  
10 NORTH CALVERT STREET  
SUITE 153  
BALTIMORE, MD 21202

EXAMINER
----------

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

47

## Office Action Summary

Application No.

10/076,948

Applicant(s)

HALTMEYER, JOHN M.

Examiner

Thomas M. Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 February 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1 is/are allowed.
- 6) ☒ Claim(s) 2-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>5/9/02</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. Claims 1-9 are pending.
2. Claim 1 is allowable.
3. Claims 2-9 are rejected.

### ***Reasons for Allowance***

4. Hammond, US patent 6463583 and “Teach Yourself Unix in a Week”, (Chapter 16, pages 420 – 449) Taylor. discloses a process for restricting unauthorized operations by a computer user, comprising:
  - Using a security executable to create a list of authorized operations for said computer user; Taylor (pages 442-443)
  - Attaching a hook function to all new processes; Hammond (Abstract) & Figure 5.
  - Employing the hook function whenever a new application is started to send message to the security executable, said message including a process id and path of the new application, where the path of the process is the thread of execution for the particular application. Hammond (Column 7, lines 54-65), and a message with the process ID is Inherent to SetWindowsHookEx function as disclosed by Hammond as a parameter, dwThreadId. (See “SetWindowsHookEx” reference, Dietmoday.com))
  - Receiving said message from the hook function and correlating to said list to determine whether the new application is authorized or not. Taylor (pages 442-443)

- Stopping the new application when the new application is not authorized. Taylor (page 445, task 16.6)

Hammond and Taylor fail to disclose:

- Using a security executable to create a list of authorized operations for said computer user.
- Answering the message by the security executable when the new application is authorized to indicate so.
- And receiving said message from the hook function at the security executable.

While it is well known in the art to create a list of authorized operations, claim 1 recites this as being performed by the security executable. Furthermore, the Security Executable is used by the Hook functions to receive messages to make a determinant as to whether or not the application is authorized to run or not. No qualifying prior art has been found to preserve this relationship as set forth by the claim. No motivation has been found to combine recitations. For this reason, independent claim 1 is allowable.

### *Claim Rejections - 35 USC § 112*

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant has recited in claim 4, and through incorporation by reference, claims 5-8:

The software system for restricting unauthorized operations by a computer user according to claim 2, wherein said first program module is attached to new processes by tying into the USER32.

The Examiner contends that the USER32 is undefined. That is, it is not explicitly stated what the USER32 is. From the specification, it appears the Applicant means “tying to the USER32” means using the system dynamic link library, USER32.dll. It is uncertain what typing into a USER32 means, or even tying into a USER32.dll. The USER32 may very well be variable or constant as well known in the art. The art of computer science often has a number of well known constants. Applicant may overcome the 112 rejection by clarifying the definition of “tying into the USER32”. Preponderance of the evidence against the prior art would appear to suggest however, that use of the USER32 means the injection code that calls for a portion of code to be executed from within a file known as USER32.dll. This stated as the prior art in Hammond, US patent 6463583, (Column 1, line 60 – Column 2, line 5). For purposes of examination, the Examiner will interpret the claims as understood in the prior art.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 2-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hammond, US patent 6463583 and “Teach Yourself Unix in a Week”, (Chapter 16, pages 420 – 449) Taylor.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over “Teach Yourself Unix in a Week”, (Chapter 16, pages 420 – 449) Taylor.

In reference to claim 2:

Hammond and “Teach Yourself Unix in a Week”, (Chapter 16, pages 420 – 449) Taylor, discloses software system for restricting unauthorized operations by a computer user, comprising:

- A first program module for automatically attaching to all new processes Hammond (Abstract) & Figure 5.

Hammond fails to disclose:

- querying an ID of each said new process;
- A second program module in communication with said first program module, said second program module building a list of allowed applications, retrieving the ID of each new process from said first program module, and terminating each process not identified on said list of allowed applications.

The Examiner notes that the limitations involving querying an ID and having retrieving the ID of each new process and terminating each process not identified on a list are well known in the art. For Example, querying for an ID of each new process is inherent with simply listing the set of processes. Task managers frequently perform this task. To avoid contention of this issue and the rejection however, the Examiner has cited the UNIX operating system utilities “Job” and “kill”, however, the Windows NT task manager or any process viewer would do the same thing. Furthermore, the fact that this application appears in UNIX would mean that a multitude of other flavors of Unix would support identical of similar commands such as BSD, Irix, and Linux variants. These commands provide an administrator the utilities to control running processes on a particular system.

Taylor discloses:

- querying an ID of each said new process; Taylor (pgs 441-443, Figure 16.2)
- A second program module in communication with said first program module, said second program module building a list of allowed applications (page 442) , retrieving the ID of each new process from said first program module (pgs 441-443, Figure 16.2), and

terminating each process not identified on said list of allowed applications, where a process is terminated when it is no longer on the list of running applications. (page 445 & page 446, step 2)

It would have been obvious to one of ordinary skill in the art at the time of invention to support the standard UNIX operations in order to provide a utility for job and process control in an operating system.

In reference to claim 3:

Hammond (Figure 3) discloses the software system for restricting unauthorized operations by a computer user according to claim 2, wherein said first program module is executable in user mode, where the hooking mechanism occurs for an Applications that run at the user level. (Figure 3, Item 62) & (Column 11, lines 35-58)

In reference to claim 4:

Hammond (Column 1, line 60 – Column 2, line 16) discloses the software system for restricting unauthorized operations by a computer user according to claim 2, wherein said first program module is attached to new processes by tying into the USER32.

In reference to claim 5:



Hammond (Column 11, lines 35-58) discloses the software system for restricting unauthorized operations by a computer user according to claim 4, wherein said first program module is a windows hook procedure, where the windows hook procedure is SetWindowsHookEx.

In reference to claim 6:

Hammond discloses the software system for restricting unauthorized operations by a computer user according to claim 5, wherein said first program module communicates with said second program module by sending a message with the process ID and path of the process being examined, where the path of the process is the thread of execution for the particular application. (Column 7, lines 54-65), and a message with the process ID is inherent to the SetWindowsHookEx function as a parameter, dwThreadId. (See “SetWindowsHookEx” reference, Dietmoday.com)

In reference to claim 8:

Taylor discloses the software system for restricting unauthorized operations by a computer user according to claim 6, wherein said second program module automatically terminates said process when not authorized, where a process is no longer authorized to run when a KILL command has been issued to is, and the UNIX subsystem enforcing the commands, terminates the process as a result. (page 445, task 16.6)

In reference to claim 9:

Taylor discloses a process for restricting unauthorized operations by computer users in a network environment, comprising the steps of:

- Monitoring all new processes that are started and determining an ID thereof, where all new processes with the process ID can be monitored and determined from the Unix job utility. (pages 442-443)
- Determining whether the ID of each started process is on said list, where the kill function determines whether the ID of a particular process . (page 445, task 16.6)
- Allowing said process to continue when its ID is on the list, where all processes that are on the list, are processes that are currently running, and therefore processes that have been allowed to persist or “continue.” (pages 442-443)
- Terminating said process when its ID is not on the list, where the termination of the said process removes it from the list. (page 445, task 16.6)

Taylor fails to explicitly disclose maintaining a list of authorized processes and IDs for each computer user in a strict sense of authorization.

However, the Examiner notes that the current list of running processes can be given by the jobs utility in the Taylor reference. The fact that these processes are running unabated means that they are in a sense, “authorized”. (pages 442-443)

### ***Conclusion***

8. The following art not relied upon is made of record:

- US PG PUB 2001/0025311 A1 Arai et al. discloses an access control system that discloses inserting a hook function into newly formed processes, and checks a list of processes to see if the newly formed process is authorized to be run. If it is not, the process is terminated, while if the process is found on the list, the process is run. This appears to be substantially similar to Applicant's invention, but was not used as prior art. MPEP 2136.03 clearly states that Foreign Priority cannot be used to establish the date for a rejection under 35 USC 102(e).
- US patent 6718414 discloses a method of inserting hook functions in processes where the operating system is running on a write protected hard drive.

9. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.


The Examiner may also be reached through email through [Thomas.Ho6@uspto.gov](mailto:Thomas.Ho6@uspto.gov)

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Application/Control Number: 10/076,948

Page 11

Art Unit: 2134

September 28<sup>th</sup>, 2005